EXAMPLES OF MORDELL'S EQUATION, II

KEITH CONRAD

1. Introduction

Using class numbers, we find all the integral solutions to some examples of Mordell's equation $y^2 = x^3 + k$ where $\mathbf{Z}[\sqrt{-k}]$ does not have unique factorization. (See also [1, Chap. 10], [2, Chap. 14], and [4, Chap. 26].)

Example 1. We will show $y^2 = x^3 - 5$ has no integral solutions, using properties of $\mathbf{Z}[\sqrt{-5}]$. In our previous discussion of Mordell's equation, we proved this result using congruences modulo 4, and then we showed how it could be established in a second way if $\mathbf{Z}[\sqrt{-5}]$ had unique factorization. But $\mathbf{Z}[\sqrt{-5}]$ does not have unique factorization, so that second proof had an error. Now we will see how our knowledge that $\mathbf{Z}[\sqrt{-5}]$ has class number 2 lets us fix the error.

Assuming $y^2 = x^3 - 5$ for integers x and y, our previous work with this equation showed x is odd, y is even, and when we write the cube x^3 as

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}) \tag{1}$$

the only common divisors of $y+\sqrt{-5}$ and $y-\sqrt{-5}$ in $\mathbf{Z}[\sqrt{-5}]$ are units. We want to conclude that $y+\sqrt{-5}$ and $y-\sqrt{-5}$ are cubes, but $\mathbf{Z}[\sqrt{-5}]$ does not have unique factorization, so our method of reaching this conclusion was in error. But now we will show that the conclusion is correct for another reason.

Pass from (1) as an equation of elements to an equation of principal ideals:

$$(x)^3 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

We will show the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime and then appeal to unique factorization of ideals. If $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are not relatively prime, they are both divisible by some prime ideal $\mathfrak{p}$. Then

$$y + \sqrt{-5} \equiv 0 \bmod \mathfrak{p}, \quad y - \sqrt{-5} \equiv 0 \bmod \mathfrak{p},$$

so subtracting gives $2\sqrt{-5} \equiv 0 \bmod \mathfrak{p}$. Thus $(2\sqrt{-5}) \subset \mathfrak{p}$, so $\mathfrak{p}|(2\sqrt{-5})$. Taking norms, $\mathrm{N}\mathfrak{p}$ divides $\mathrm{N}(2\sqrt{-5}) = 20$. Also $\mathrm{N}\mathfrak{p}$ divides $\mathrm{N}(y + \sqrt{-5}) = y^2 + 5$, which is odd, so $\mathrm{N}\mathfrak{p} = 5$. If $\mathrm{N}\mathfrak{p} = 5$ then 5 divides $y^2 + 5$, so $5|y$. Then $x^3 = y^2 + 5 \equiv 0 \bmod 5$, so $x \equiv 0 \bmod 5$, so $5 = x^3 - y^2 \equiv 0 \bmod 25$, which is false. Thus the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ are relatively prime.

Since the ideals $(y + \sqrt{-5})$ and $(y - \sqrt{-5})$ multiply to a cube and are relatively prime, they are each cubes:

$$(y + \sqrt{-5}) = \mathfrak{a}^3, \quad (y - \sqrt{-5}) = \mathfrak{b}^3.$$

Passing to the ideal class group, $[\mathfrak{a}]^3$ is principal, so $[\mathfrak{a}]$ has order dividing 3. Since the class group has size $h = 2$, $[\mathfrak{a}]$ has order 1, which means $\mathfrak{a}$ is principal, say $\mathfrak{a} = (\alpha)$. Therefore

$(y+\sqrt{-5}) = (\alpha)^3 = (\alpha^3)$, so $y+\sqrt{-5} = u\alpha^3$, where $u \in \mathbf{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Since ± 1 are both cubes, we can absorb them into α and thus write

$$y + \sqrt{-5} = \alpha^3.$$

Now the proof can be finished up just as we did it before under the (false) assumption that $\mathbf{Z}[\sqrt{-5}]$ has unique factorization.

The key point in this treatment of $y^2 = x^3 - 5$ is that if $\mathfrak{a}^3$ is principal and the class number is prime to 3 then $\mathfrak{a}$ is principal. We don't need to have class number 1. To reinforce this, let's use that idea in another example.

Example 2. We will show the only integral solutions to $y^2 = x^3 + 2$ are $(x, y) = (-1, \pm 1)$. (There are infinitely many rational solutions, one example being $(17/4, 71/8)$.) While it is natural to first write $x^3 = y^2 - 2$ and then factor the right side by working in $\mathbf{Z}[\sqrt{2}]$, there is an infinite unit group for $\mathbf{Z}[\sqrt{2}]$, which would lead to a multi-case consideration. Instead we will do a change of variables and work in the imaginary quadratic ring $\mathbf{Z}[\sqrt{-6}]$. (This method is due to A. Brauer.)

If x is even then $y^2 \equiv 2 \bmod 8$, which has no solution. Thus x is odd, so y^2 is odd, so y is odd.

Set $x = z - 1$, so $y^2 = (z-1)^3 + 2 = z^3 - 3z^2 + 3z + 1$. Then $(y, z) = 1$ and

$$y^2 + 6z^2 = z^3 + 3z^2 + 3z + 1 = (z+1)^3. \tag{2}$$

In $\mathbf{Z}[\sqrt{-6}]$ we factor this as

$$(y + \sqrt{-6}z)(y - \sqrt{-6}z) = (z+1)^3. \tag{3}$$

The class number of $\mathbf{Q}(\sqrt{-6})$ is 2, so let's treat equation (3) as an equation of ideals rather than elements. To show the ideals $(y + \sqrt{-6}z)$ and $(y - \sqrt{-6}z)$ are relatively prime, suppose they have a common prime ideal factor $\mathfrak{p}$:

$$y + \sqrt{-6}z \equiv 0 \bmod \mathfrak{p}, \quad y - \sqrt{-6}z \equiv 0 \bmod \mathfrak{p}.$$

We will get a contradiction. Adding and subtracting the congruences, $2y \equiv 0 \bmod \mathfrak{p}$ and $2\sqrt{-6}z \equiv 0 \bmod \mathfrak{p}$. Thus $(2y) \subset \mathfrak{p}$ and $(2\sqrt{-6}z) \subset \mathfrak{p}$. Taking norms, $\mathrm{N}\mathfrak{p}$ divides $4y^2$ and $24z^2$. Also $\mathrm{N}\mathfrak{p}$ divides $\mathrm{N}(y + \sqrt{-6}z) = y^2 + 6z^2$, which is odd, so $\mathrm{N}\mathfrak{p}$ is odd. Therefore $\mathrm{N}\mathfrak{p}$ divides y^2 and $3z^2$. Since y and z are relatively prime, $\mathrm{N}\mathfrak{p}|3$, so $\mathrm{N}\mathfrak{p} = 3$. Therefore $3|y^2$, so y is a multiple of 3 and $x^3 = y^2 - 2 \equiv 7 \bmod 9$. The only cubes mod 9 and 0, 1, and -1, so we have a contradiction.

Since the class number 2 is relatively prime to 3, from (3) as an equation of ideals the factors $(y + \sqrt{-6}z)$ and $(y - \sqrt{-6}z)$ are both cubes of ideals, and by the same argument as in $\mathbf{Z}[\sqrt{-5}]$ the elements $y + \sqrt{-6}z$ and $y - \sqrt{-6}z$ are both cubes in $\mathbf{Z}[\sqrt{-6}]$. Write

$$y + \sqrt{-6}z = (a + b\sqrt{-6})^3. \tag{4}$$

Taking norms of both sides in (4), $y^2 + 6z^2 = (a^2 + 6b^2)^3$, and comparing this with (2) gives us $z + 1 = a^2 + 6b^2$. Equating the imaginary parts in (4), $z = 3a^2b - 6b^3$, so

$$3a^2b - 6b^3 = a^2 + 6b^2 - 1.$$

Putting the a-free terms on the right,

$$a^2(3b - 1) = 6b^3 + 6b^2 - 1.$$

Multiply by 9 and reduce modulo $3b - 1$:

$$0 \equiv 2 + 6 - 9 = -1 \bmod 3b - 1.$$

The only moduli where $0 \equiv -1$ are ± 1, so $3b-1$ is 1 or -1. The first choice is not possible, while the second leads to $b = 0$. Then $z = 3a^2b - 6b^3 = 0$, so $x = z - 1 = -1$ and $y^2 = x^3 + 2 = 1$, so $y = \pm 1$.

Example 3. The equation $y^2 = x^3 - 26$ has four integral solutions: $(3, \pm 1)$ and $(35, \pm 207)$. We will use algebraic number theory to prove these are the only integral solutions.

If x is even then $y^2 \equiv -26 \equiv 6 \bmod 8$, but 6 mod 8 is not a square. Therefore x is odd, so y is odd too.

Rewrite the equation as

$$x^3 = y^2 + 26 = (y + \sqrt{-26})(y - \sqrt{-26})$$

and pass to principal ideals:

$$(x)^3 = (y + \sqrt{-26})(y - \sqrt{-26}).$$

Step 1: The ideals $(y + \sqrt{-26})$ and $(y - \sqrt{-26})$ are relatively prime.

Suppose the ideals have a common prime ideal factor $\mathfrak{p}$, so

$$y + \sqrt{-26} \equiv 0 \bmod \mathfrak{p}, \quad y - \sqrt{-26} \equiv 0 \bmod \mathfrak{p}.$$

Subtracting, $2\sqrt{-26} \equiv 0 \bmod \mathfrak{p}$, so $\mathfrak{p} | (2)(\sqrt{-26})$. How do (2) and $(\sqrt{-26})$ factor in $\mathbf{Z}[\sqrt{-26}]$?

p	$T^2 + 26 \bmod p$	(p)
2	T^2	$\mathfrak{p}_2^2$
3	$(T+1)(T-1)$	$\mathfrak{p}_3\mathfrak{p}_3'$
13	T^2	$\mathfrak{p}_{13}^2$

TABLE 1.

By Table 1, (2) and (13) are both squares of prime ideals. Since $\mathrm{N}(\sqrt{-26}) = 26 = 2 \cdot 13$, $(\sqrt{-26}) = \mathfrak{p}_2\mathfrak{p}_{13}$. Therefore $\mathfrak{p} = \mathfrak{p}_2$ or $\mathfrak{p} = \mathfrak{p}_{13}$. If $\mathfrak{p} = \mathfrak{p}_2$ then from $y + \sqrt{-26} \equiv 0 \bmod \mathfrak{p}_2$ we get $y \equiv 0 \bmod \mathfrak{p}_2$, so y is even, so x is even. Then $26 = x^3 - y^2 \equiv 0 \bmod 4$, a contradiction. If $\mathfrak{p} = \mathfrak{p}_{13}$ then we get a similar contradiction (check). Thus the ideals $(y + \sqrt{-26})$ and $(y - \sqrt{-26})$ are relatively prime.

Relatively prime ideals multiply to a cube only when each is a cube, so

$$(y + \sqrt{-26}) = \mathfrak{a}^3 \tag{5}$$

for some ideal $\mathfrak{a}$. Since $\mathfrak{a}$ has a principal cube, $[\mathfrak{a}]$ has order 1 or 3.

Step 2: The class group of $\mathbf{Q}(\sqrt{-26})$ is cyclic of order 6.

The Minkowski bound is

$$\left(\frac{4}{\pi}\right)^2 \frac{n!}{n^n} \sqrt{|\operatorname{disc}(K)|} = \frac{2\sqrt{26}}{\pi} \approx 3.24.$$

So the class group is generated by the prime ideals of norm 2 and 3. Since $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ (see Table 1), $[\mathfrak{p}_2]$ and either $[\mathfrak{p}_3]$ or $[\mathfrak{p}_3']$ generate the class group. No element of $\mathbf{Z}[\sqrt{-26}]$ has norm 2 or 3, so $\mathfrak{p}_2$, $\mathfrak{p}_3$, and $\mathfrak{p}_3'$ are nonprincipal. Since $\mathfrak{p}_2^2 = (2)$, $[\mathfrak{p}_2]$ has order 2. Since $\mathrm{N}(1 + \sqrt{-26}) = 27$ and (3) does not divide $(1 + \sqrt{-26})$, $(1 + \sqrt{-26})$ is either $\mathfrak{p}_3^3$ or $\mathfrak{p}_3'^3$. Therefore the ideal classes $[\mathfrak{p}_3]$ and $[\mathfrak{p}_3']$ (which are inverses of each other) have order 3, so the class group is abelian of order 6, hence cyclic.

In particular, the ideal classes of order 3 are $[\mathfrak{p}_3]$ and $[\mathfrak{p}_3']$.

Case 1: The ideal $\mathfrak{a}$ is principal.

When $\mathfrak{a}$ is principal, write $\mathfrak{a} = (\alpha)$, so $(y + \sqrt{-26}) = (\alpha^3)$. The units in $\mathbf{Z}[\sqrt{-26}]$ are ± 1, which are both cubes, so after perhaps changing α by a sign we get

$$y + \sqrt{-26} = \alpha^3.$$

This is exactly the equation we derived in our previous look at the equation $y^2 = x^3 - 26$, under the false assumption that $\mathbf{Z}[\sqrt{-26}]$ has unique factorization. The calculations used there can now be applied here to derive $y = \pm 207$.

Case 2: The ideal $\mathfrak{a}$ is nonprincipal. So $[\mathfrak{a}]$ has order 3.

Having already found the possibility $y = \pm 207$, now we expect to show $y = \pm 1$. When $\mathfrak{a}$ is nonprincipal, either $[\mathfrak{a}] = [\mathfrak{p}_3] = [\mathfrak{p}_3']^{-1}$ or $[\mathfrak{a}] = [\mathfrak{p}_3'] = [\mathfrak{p}_3]^{-1}$, so $\mathfrak{a}\mathfrak{p}_3'$ or $\mathfrak{a}\mathfrak{p}_3$ is principal. Let $\mathfrak{p}_3$ denote the ideal with norm 3 such that $\mathfrak{a}\mathfrak{p}_3$ is principal. Multiplying both sides of the equation (5) by $\mathfrak{p}_3^3$,

$$\mathfrak{p}_3^3(y + \sqrt{-26}) = (\alpha)^3$$

for some $\alpha \in \mathbf{Z}[\sqrt{-26}]$. The ideal $\mathfrak{p}_3^3$ is either $(1 + \sqrt{-26})$ or $(1 - \sqrt{-26})$, so

$$(1 \pm \sqrt{-26})(y + \sqrt{-26}) = (\alpha^3).$$

If this holds with one choice of sign then it holds with the other by conjugating everything (and then replacing y with $-y$). So it suffices to focus on

$$(1 + \sqrt{-26})(y + \sqrt{-26}) = (\alpha^3). \tag{6}$$

and show $y = \pm 1$. In fact, we will see that $y = -1$.

Since units in $\mathbf{Z}[\sqrt{-26}]$ are cubes, (6) implies the equation of elements

$$(1 + \sqrt{-26})(y + \sqrt{-26}) = (a + b\sqrt{-26})^3$$

for some integers a and b. Equating real and imaginary parts,

$$y - 26 = a^3 - 78ab^2, \quad y + 1 = 3a^2b - 26b^3. \tag{7}$$

Subtracting the first equation from the second,

$$27 = 3a^2b - 26b^3 - a^3 + 78ab^2. \tag{8}$$

Reducing (8) modulo 3 shows $0 \equiv b^3 - a^3 \bmod 3$, so $b \equiv a \bmod 3$. Write $b = a + 3c$ and substitute into (8):

$$27 = 3a^2(a + 3c) - 26(a + 3c)^3 - a^3 + 78a(a + 3c)^2 = 27(2a^3 + 9a^2c - 26c^3).$$

Hence

$$1 = 2a^3 + 9a^2c - 26c^3. \tag{9}$$

We are going to show the only integral solution to (9) is $a = -3$ and $c = 1$. Then $b = a + 3c = 0$ and (7) implies $y = -1$, so $x^3 = 27$, hence $x = 3$.

In (9), make the invertible $\mathbf{Z}$-linear change of variables $m = c$ and $n = a + 3c$ (so $a = n - 3m$). This turns (9) into

$$1 = m^3 - 9mn^2 + 2n^3. \tag{10}$$

We will show the only integral solution of (10) is $m = 1$, $n = 0$ (so $a = -3$ and $c = 1$, as desired). There are infinitely many rational solutions to (10), such as $(m, n) = (1, 9/2)$ and $(m, n) = (-11/5, -4/5)$. We care only about integral solutions.

The right side of (10) is the norm from a cubic field. Set $F = \mathbf{Q}(\gamma)$ where γ is a root of $f(T) = T^3 - 9T - 2$. This cubic is irreducible, so $[F : \mathbf{Q}] = 3$. A short calculation shows $\mathrm{N}_{F/\mathbf{Q}}(r + s\gamma) = r^3 - 9rs^2 + 2s^3$ for rational r and s, so (10) is the same as

$$\mathrm{N}_{F/\mathbf{Q}}(m + n\gamma) = 1,$$

which means $m + n\gamma$ is a unit in $\mathbf{Z}[\gamma]$. We are searching for units of norm 1 in $\mathbf{Z}[\gamma]$ with γ^2-coefficient equal to 0. That is a strong constraint on a unit.

From now on our attention is focused on the cubic field F, not on the quadratic field $\mathbf{Q}(\sqrt{-26})$.

Step 7: The ring of integers of $F = \mathbf{Q}(\gamma)$ is $\mathbf{Z}[\gamma]$.

Since $\mathrm{disc}(f(T)) = 2^3 3^3 13 = [\mathcal{O}_F : \mathbf{Z}[\gamma]]^2 \mathrm{disc}(\mathcal{O}_F)$, we will show 2, 3, and 13 don't divide $[\mathcal{O}_F : \mathbf{Z}[\gamma]]$. We have $\mathrm{disc}(f(T)) = [\mathcal{O}_F : \mathbf{Z}[\gamma]]^2 \mathrm{disc}(F)$. Because 13 only divides $\mathrm{disc}(f(T))$ once, it doesn't divide $[\mathcal{O}_F : \mathbf{Z}[\gamma]]$.

$$f(T - 1) = T^3 - 3T^2 - 6T + 6,$$

which is Eisenstein at 3, 3 is totally ramified in $\mathcal{O}_F$ and 3 does not divide $[\mathcal{O}_F : \mathbf{Z}[\gamma + 1]] = [\mathcal{O}_F : \mathbf{Z}[\gamma]]$.

The only possibility left is $[\mathcal{O}_F : \mathbf{Z}[\gamma]] = 1$ or 2. If the index is 2 then $\mathrm{disc}(\mathcal{O}_F) = 2 \cdot 3^3 \cdot 13 \equiv 2 \bmod 4$, which violates Stickelberger's congruence (which says the discriminant of a number field is 0 or 1 mod 4). Therefore $[\mathcal{O}_F : \mathbf{Z}[\gamma]] = 1$.

Step 8: Applying the unit theorem.

Returning to (10), we want to show the only unit in $\mathbf{Z}[\gamma] = \mathcal{O}_F$ with norm 1 having γ^2-coefficient 0 is 1. Since $\mathrm{N}_{F/\mathbf{Q}}(-\beta) = -\mathrm{N}_{F/\mathbf{Q}}(\beta)$, we can just as well show the only units having γ^2-coefficient 0 are ± 1.

Since $r_1(F) = 3$ and $r_2(F) = 0$, $\mathcal{O}_F^\times$ has rank 2: $\mathcal{O}_F^\times = \pm\varepsilon_1^{\mathbf{Z}}\varepsilon_2^{\mathbf{Z}}$.

We will present candidates for fundamental units. By PARI, a set of fundamental units is $1 + 9\gamma + 3\gamma^2$ and $1 + 4\gamma - 2\gamma^2$.

Try Skolem's method for $p = 2$. See [3, p. 204].

This also tells us about power bases in $\mathcal{O}_F$. Since

$$[\mathbf{Z}[\gamma] : \mathbf{Z}[x\gamma + y\gamma^2]] = |x^3 - 9xy^2 - 2y^3|,$$

for $x\gamma + y\gamma^2$ to generate a power basis we need

$$x^3 - 9xy^2 - 2y^3 = \pm 1.$$

The left side is homogeneous of odd degree, so it's enough to focus on

$$x^3 - 9xy^2 - 2y^3 = 1.$$

The only $\mathbf{Z}$-solution is $(x, y) = (1, 0)$, so the only power basis of $\mathbf{Z}[\gamma]$ is $\{1, \gamma, \gamma^2\}$.

References

[1] W. W. Adams, L. J. Goldstein, "Introduction to Number Theory," Prentice Hall, 1973.

[2] S. Alaca, K. S. Williams, "Introductory Algebraic Number Theory," Cambridge Univ. Press, 2004.

[3] F. B. Coghlan and N. M. Stephens, *The Diophantine Equation* $x^3 - y^2 = k$, in: "Computers in Number Theory," Academic Press, London, 1971.

[4] L. Mordell, "Diophantine Equations," Academic Press, 1969.